What is claimed is:

1. A personal digital identifier device for controlling access to a computer network, said network comprising a plurality of workstations each having a base unit associated therewith, said base unit being configured for wireless communications with said personal digital identifier device, and said network further comprising a central server utilizing a security manager component and network storage, said security manager component associated with a private key and a corresponding public key and said network storage containing a public key corresponding to a private key held by said personal digital identifier device, said personal digital identifier device being lightweight, configured for wearing and/or carrying by a user registered thereto and comprising:

(a) a wireless communications component comprising a transceiver for communicating with said base unit;

(b) a biometric acquisition component for obtaining a user's input biometric and producing a digital representation thereof;

(c) a processor configured for communicating with said transceiver and said biometric component and operable for:

(i) evaluating whether a template derived from said digital representation corresponds to a master template derived from a user's biometric digital representation previously produced by said biometric component and generating a matching signal when such a correspondence is determined;

(ii) generating said private key held by said personal digital identifier device and said public key corresponding thereto and outputting said generated public key for transmission by said transceiver;

(iii) producing a digital signature using said private key; and,

(iv) verifying, using said public key for said private key associated with said security manager component, that the source of an encrypted message ostensibly received from said security manager is said security manager component;

(d) secure storage containing said master template of a user's biometric, said generated private key and said public key for said private key associated with said security manager component;

(e) a power source; and,

(f) a housing,

said personal digital identifier device being configured for producing, using said generated private key, a digitally signed challenge response message following said generating of said matching signal in response to a challenge message received from said security manager component and for transmitting said response message, and said personal digital identifier device being configured to prevent transmission of any of said master template of a user's biometric and said private key.

2. A personal digital identifier device according to claim 1 wherein said biometric component includes a transducer.

3. A personal digital identifier device according to claim 1 wherein a response signal is automatically transmitted from said transceiver in response to a signal received by said transceiver from one said base unit.

4. A personal digital identifier device according to claim 1 wherein all data held in said secure storage is by itself non-identifiable of said user.

5. A personal digital identifier device according to claim 2 wherein said transducer comprises a solid state fingerprint sensor.

6. A personal digital identifier device according to claim 5 wherein said transceiver transmits and receives optical signals.

7. A personal digital identifier device according to claim 6 wherein said

transceiver transmits and receives radio frequency signals.

8. A personal digital identifier device according to claim 1 in combination with a device holder wherein said device holder is configured to co-operate with said housing of said personal digital identifier device such that said personal digital identifier device is held by said holder device when it is appropriately positioned relative to said holder device, said device holder comprising a communications connector for communicatively coupling said personal digital identifier device directly to one said workstation when said personal digital identifier device is held by said device holder.

9. A security system for controlling access to a computer network at a network access point comprising a workstation, said system comprising:

A. a personal digital identifier device comprising:

(a) a wireless communications component comprising a transceiver;

(b) a biometric acquisition component for obtaining a user's input biometric and producing a digital representation thereof;

(c) a processor configured for communicating with said transceiver and said biometric component and operable for:

(i) evaluating whether a template derived from said digital representation corresponds to a master template derived from a user's biometric digital representation previously produced by said biometric component and generating a matching signal when such a correspondence is determined;

(ii) generating a private key to be held by said personal digital identifier device and a public key corresponding thereto and outputting said generated public key for transmission by said transceiver;

(iii) producing a digital signature using said private key; and,

(iv) verifying that an encrypted received message is from a security manager component using a public key for a private key associated with said security manager component; and,

(d) secure storage containing said master template of a user's biometric, said generated private key and said public key for said private key associated with said security manager component,

said personal digital identifier device being configured for producing, using said generated private key, a digitally signed challenge response message following said generating of said matching signal in response to a challenge received from said security manager component and for transmitting said response message, and said personal digital identifier device being configured to prevent transmission of any of said master template of a user's biometric and said private key;

B. a base unit associated with said workstation and configured for initiating and maintaining wireless communications with said personal digital identifier device, said communications extending over an area defined by an envelope associated with said workstation; and,

C. a central server having access to network storage and utilizing said security manager component and said personal digital identifier device for authenticating said user, said network storage containing a public key corresponding to said private key generated by said personal digital identifier device.

10. A security system according to claim 9 wherein said biometric component includes a transducer.

11. A security system according to claim 9 wherein said workstation is a personal computer.

12. A security system according to claim 9 wherein said base unit regularly

transmits a first signal to said personal digital identifier device and said personal digital identifier device automatically transmits a response signal in response thereto when said personal digital identifier device is within said envelope.

13. A security system according to claim 12 comprising a plurality of said personal digital identifier devices, a plurality of workstations and a plurality of base units wherein a base unit is associated with each said workstation, each said base unit transmitting a polling signal to each said personal digital identifier device within said base unit's associated envelope following said base unit's receipt of said response signal from each said personal digital identifier device.

14. A security system according to claim 9 wherein all data held in said secure storage of said personal digital identifier device is by itself non-identifiable of said user.

15. A security system according to claim 9 wherein said network storage includes data identifiable of said user for display on a screen of said workstation when said user's personal identification device is located within said envelope.

16. A security system according to claim 9 wherein said envelope has a shape and area which are configured to encompass those locations proximate to said workstation at which an observer may read and/or understand information displayed on a screen of said workstation.

17. A method for controlling access to a computer network in which workstations provide points of access to said network, said network including a central server communicating with said workstations and secure network storage, and a base unit configured for initiating and maintaining wireless communications with a portable personal digital identifier device carried or held by a user being associated with each said workstation, said wireless communications extending over an area

defined by an envelope associated with said workstation, said method comprising the steps:

(a) on registration of a portable personal digital identifier device to a user, within said portable personal digital identifier device: receiving an input biometric of said user, producing a digital representation thereof, deriving from said digital representation a master template, securely maintaining said master template in storage, generating and securely maintaining in said storage a private key, generating a public key corresponding to said generated private key and providing said generated public key for storage in said network storage and receiving and storing in said storage a public key for a private key associated with a network security manager component ;

(b) transmitting a first signal from a base unit associated with one said workstation to said personal digital identifier device and automatically transmitting from said personal digital identifier device a response signal establishing communications between said base unit and said personal digital identifier device in response to said first signal when said personal digital identifier device is within said envelope;

(c) receiving at said personal digital identifier device a digitally signed challenge message ostensibly from said network security manager component and verifying within said personal digital identifier device the origin of said challenge using said public key for said private key associated with said security manager component;

(d) acquiring on said portable personal digital identifier device an input biometric of said user, producing a digital representation thereof and deriving from said digital representation a biometric template;

(e) evaluating within said portable personal digital identifier device whether said biometric template corresponds to said master template and generating a matching signal when such a correspondence is determined;

(f) producing within said personal digital identifier device, using said generated private key, a digitally signed challenge response message following said generating of said matching signal in response to said challenge message and transmitting said response message to said security manager component to authenticate said user; and,

(g) permitting said authenticated user to access said computer network through said workstation.

18. A method according to claim 17 and further comprising configuring the shape and area of said envelope to encompass those locations proximate to said workstation at which an observer may read and/or understand information displayed on a screen of said workstation.

19. A method according to claim 17 and further comprising, following said base unit's receipt of said response signal from said personal digital identifier device, transmitting from said base unit a polling signal to said personal digital identifier device for determining whether said personal digital identifier device remains located within said base unit's associated envelope.

20. A method according to claim 17 and further comprising displaying on a screen of said workstation data identifying said user when said user is identified.

21. A method according to claim 17 and further comprising initially registering said user by a registrar in the presence of a guarantor, said registrar and guarantor each being a registered user of the computer network and said registrar having access to the computer network and verified by said security manager component to have registration privileges, and requiring: that said guarantor provide to said security manager component a biometrically digitally signed message to authenticate said guarantor and that each of said registrar, guarantor and user remain within said envelope during said registering of said user.

22. A method according to claim 17 whereby a policy manager component may direct that the screen of said workstation be blanked out when a new personal digital identifier device moves to a location within said envelope until such time as the user registered to said personal digital identifier device is biometrically identified.